Journal of Combinatorial Theory, Series A **93**, 112–124 (2001)
doi:10.1006/jcta.2000.3068, available online at http://www.idealibrary.com on IDEAL®

# Explicit Constructions of Perfect Hash Families from Algebraic Curves over Finite Fields[1]

Huaxiong Wang[2]

*School of Information Technology and Computer Science, University of Wollongong, Northfields Avenue, Wollongong, NSW 2522, Australia*
E-mail: huaxiong@uow.edu.au

and

Chaoping Xing[3]

*Department of Mathematics, National University of Singapore,*



*Communicated by the Managing Editors*

Received October 18, 1999

Let $A$ be a set of order $n$ and $B$ be a set of order $m$. An $(n, m, w)$-*perfect hash family* is a set $\mathscr{H}$ of functions from $A$ to $B$ such that for any $X \subseteq A$ with $|X| = w$, there exists an element $h \in \mathscr{H}$ such that $h$ is one-to-one when restricted to $X$. Perfect hash families have many applications to computer science, such as database management, circuit complexity theory and cryptography. In this paper, we provide explicit constructions of perfect hash families based on algebraic curves over finite fields. In particular, using the Garcia–Stichtenoth curves, we obtain infinite classes of $(n, m, w)$-perfect hash families with $|\mathscr{H}| = O(\log n)$ for fixed $m$ and $w$, which are among the most efficient explicit constructions for perfect hash families known in the literature. We also exhibit examples to show the efficiency of the new constructions and their applications to the constructions of cover-free families. 

*Key Words:* algebraic curves; perfect hash family; cover-free family.

## 1. INTRODUCTION

Let $n$ and $m$ be integers such that $2 \leqslant m \leqslant n$. Let $A$ be a set of order $n$ and let $B$ be a set of order $m$. A *hash function* is a function $h$ from $A$ to $B$.

[1] Research of the second author is support by the NUS grant R-146-000-018-112.

[2] Most of this work was carried out when the author was with Department of Computer Science, School of Computing, National University of Singapore.

[3] To whom correspondence should be addressed.



0097-3165/01 $35.00

We say a hash function $h: A \to B$ is *perfect* on a subset $X \subseteq A$ if $h$ is injective when restricted on $X$. Let $w$ be an integer such that $2 \leqslant w \leqslant m$, and let $\mathscr{H} \subseteq \{h: A \to B\}$. We say $\mathscr{H}$ is an $(n, m, w)$-*perfect hash family* if for any $X \subseteq A$ with $|X| = w$ there exists at least one element $h \in \mathscr{H}$ such that $h$ is perfect on $X$.

Perfect hash families originally arose as part of compiler design—see Mehlhorn [16] for a summary of the early results in this area. They have applications to operating system, language translation system, hypertext, hypermedia, file managers, and information retrieval system—see Czech *et al.* [8] for survey of recent results. More recently, they have found numerous applications to cryptography, for example, to broadcast encryption [11], secret sharing [5], key distribution patterns, cover-free families and secure frameproof codes [20].

We will follow the notation in [3]. Let $PHF(N; n, m, w)$ denote an $(n, m, w)$-perfect hash family with $|\mathscr{H}| = N$, and let $N(n, m, w)$ denote the minimum $N$ for which a $PHF(N; n, m, w)$ exists. We are interested in determining these values. In particular, we are interested in the asymptotic behavior of $N(n, m, w)$ as a function of $n$ when $m$ and $w$ are fixed. Bounds on $N(n, m, w)$ have been studied by numerous authors (see, for example, [3, 4, 6, 12, 16, 21]). In particular, it is proved in [16] that for fixed $m$ and $w$, $N(n, m, w)$ is $\Theta(\log n)$. However, this existence result is non-constructive. It was believed that it is difficult to give explicit constructions that are asymptotically as good as the above existence result. Efforts have been thus made to give explicit constructions which, while not achieving the above bound, are much more efficient compared to the trivial solution.

The goal of this paper is to explore the explicit constructions for perfect hash families from algebraic curves over finite fields. We present infinite classes of perfect hash families from some specific algebraic curves with many rational points. In particular, using a simple product type construction due to Blackburn *et al.* [4, 5], and applying our construction based on the Garcia–Stichtenoth curves, for any given integers $m$ and $w$ we are able to construct infinite classes of perfect hash families in which $N$ is $O(\log n)$. This is the explicit construction of perfect hash families with the best asymptotic behavior previously known in the literature. We also exhibit examples to make direct comparisons with previously known constructions, and as an application we provide new explicit constructions for cover-free families with the best parameters known previously.

The paper is organized as follows. In Section 2 we briefly review the bounds and explicit results of constructions for perfect hash families. In Section 3 we present our construction from algebraic curves over finite fields and prove the main result of the paper. In Section 4 we give an example to illustrate the efficiency of our new construction; and we also show that our results provide more efficient and explicit constructions of

cover-free families. In Section 5 we conclude our paper and discuss linear perfect hash families.

## 2. PREVIOUS RESULTS ON PERFECT HASH FAMILIES

In this section, we will briefly review some previous existence results for and previous constructions of perfect hash families.

As before, $N(n, m, w)$ denotes the smallest value $N$ for which a $PHF(N; n, w)$ exists. All logarithms in this paper are to the base 2, unless otherwise indicated. We start with lower bounds for $N(n, m, w)$. The first result is due to Fredman and Komlòs [12]:

THEOREM 2.1.

$$N(n, m, w) \geqslant \frac{\binom{n-1}{w-2} m^{w-2} \log(n-w+2)}{\binom{m-1}{w-2} n^{w-2} \log(m-w+2)}.$$

As noted in [4], this lower bound is approximately equal to

$$\frac{m^{w-2}}{m(m-1)(m-2)\cdots(m-(w-1))} \frac{\log n}{\log(m-w+2)}$$

as $n \to \infty$ with $w$ and $m$ fixed.

A weaker bound, due to Mehlhorn [16], is

THEOREM 2.2. $N(n, m, w) \geqslant \frac{\log n}{\log m}$.

This bound can be met when $w = 2$. In fact, there exists an explicit construction such that $N(n, m, 2) = \lceil \frac{\log n}{\log m} \rceil$ for any integers $n \geqslant m$, where $\lceil v \rceil$ denotes the least integer greater than or equal to the real number $v$.

Using an elementary probabilistic argument, the following non-constructive upper bound for $N(n, m, w)$ was proved by Mehlhorn [16].

THEOREM 2.3.

$$N(n, m, w) \leqslant \left\lceil \frac{\log\binom{n}{w}}{\log(m^w) - \log\left(m^w - w!\binom{m}{w}\right)} \right\rceil.$$

Straightforward approximations, using Theorem 2.3, yield the following corollary.

COROLLARY 2.1 [16]. $N(n, m, w) \leqslant \lceil we^{w^2/m} \log n \rceil$.

From Theorem 2.2 and Corollary 2.4, it follows that for fixed $m$ and $w$, $N(n, m, w)$ as a function on $n$ is $\Theta(\log n)$. However, the above existence results are non-constructive, and it was believed that it is difficult to give explicit constructions that are asymptotically as good as Corollary 2.1.

Efforts have been made to provide explicit constructions which are much more efficient compared to the trivial solutions or quite reasonable compared to the asymptotically optimal bounds. Most known explicit perfect hash families are constructed from error-correcting codes by Alon [1], resolvable balanced incomplete block designs by Brickell [7], and various inductive techniques by Atici *et al.* [3]. For a good survey of this subject we refer readers to Blackburn [4].

In [3], Atici *et al.* provide various recursive methods resulting in explicit constructions of $PHF(N; n, m, w)$ in which $N$ is a polynomial function of $\log n$ for fixed $m$ and $w$. Recently, Stinson *et al.* [21] employ some combinatorial techniques to generalize and improve results from [3]. For given $m$ and $w$, they construct $PHF(N; n, m, w)$ in which $N$ is $O(C^{\log^*(n)} \log n)$, where $C$ is a constant only depending on $w$, and log* is function from $\mathbf{Z}^+$ to $\mathbf{Z}^+$ recursively defined as $\log^*(1) = 1$, $\log^*(n) = \log^*(\lceil \log n \rceil) + 1$ for $n > 1$.

Blackburn and Wild [6] introduce and study the *linear perfect hash families*, they show that there exist explicit constructions for $PHF(N; n, m, w)$ in which $N = (w-1) \log n / \log m$. Although the classes of linear perfect hash families are of interest in their own right, their constructions are, however, quite restrictive in general, since they require $m$ to be a prime power and to be very large compared to $w$ and $N$.

As we will show in Section 3, using algebraic curves, for any fixed integers $w$ and $m$ we can obtain explicit constructions of $PHF(N; n, m, w)$'s with $N = C \log n$, where $C$ is a constant depending only on $w$ and $m$ as $n$ tends to $\infty$.

## 3. CONSTRUCTIONS

In this section, we describe a construction of perfect hash families based on algebraic curves over finite fields. Before starting our construction, we need to introduce some concepts and notations that are essential for the construction. For further results on algebraic curves over finite fields, we refer to [19, 22].

We fix some notations for this section.

$q$—power of a prime;

$\mathbf{F}_q$—the finite field of $q$ elements;

$\mathcal{X}$—a projective, absolutely irreducible, complete algebraic curve defined over $\mathbf{F}_q$. We simply say that $\mathcal{X}/\mathbf{F}_q$ is an algebraic curve;

$g = g(\mathcal{X})$—the genus of $\mathcal{X}$;

$\mathbf{F}_q(\mathcal{X})$—the function field of $\mathcal{X}$;

$\mathcal{X}(\mathbf{F}_q)$—the set of all $\mathbf{F}_q$-rational points on $\mathcal{X}$ with all coordinates belonging to $\mathbf{F}_q$.

A divisor $G$ of $\mathcal{X}$ is called *rational* if

$$G^\sigma = G$$

for any automorphism $\sigma \in \mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q)$, where $\bar{\mathbf{F}}_q$ is a fixed algebraic closure of $\mathbf{F}_q$ and $\mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q)$ is the Galois group of $\bar{\mathbf{F}}_q/\mathbf{F}_q$. In this paper we always mean a rational divisor whenever a divisor is mentioned.

We write $v_P$ for the normalized discrete valuation corresponding to the point $P$ of $\mathcal{X}$. Let $x \in \mathbf{F}_q(\mathcal{X})\backslash\{0\}$ and denote by $Z(x)$, respectively $N(x)$, the set of zeros, respectively poles, of $x$. We define the *zero divisor* of $x$ by

$$(x)_0 = \sum_{P \in Z(x)} v_P(x)\, P \tag{1}$$

and the *pole divisor* of $x$ by

$$(x)_\infty = \sum_{P \in N(x)} (-v_P(x))\, P. \tag{2}$$

Then $(x)_0$ and $(x)_\infty$ are both rational divisors. Furthermore, the *principal divisor* of $x$ is given by

$$\mathrm{div}(x) = (x)_0 - (x)_\infty. \tag{3}$$

The degree of $\mathrm{div}(x)$ is equal to zero, i.e.,

$$\deg((x)_0) = \sum_{P \in Z(x)} v_P(x) = \sum_{P \in N(x)} (-v_P(x)) = \deg((x)_\infty). \tag{4}$$

For an arbitrary divisor $G = \sum m_P P$ of $\mathcal{X}$, we denote by $v_P(G)$ the coefficient $m_P$ of $P$. Then

$$G = \sum v_P(G)\, P.$$

For such a divisor $G$ we form the vector space

$$\mathscr{L}(G) = \{x \in \mathbf{F}_q(\mathscr{X}) \backslash \{0\} : \operatorname{div}(x) + G \geqslant 0\} \cup \{0\}.$$

Then $\mathscr{L}(G)$ is a finite-dimensional vector space over $\mathbf{F}_q$, and we denote its dimension by $\ell(G)$. By the Riemann–Roch theorem (see [19, 22]), we have

$$\ell(G) \geqslant \deg(G) + 1 - g, \tag{5}$$

and equality holds if $\deg(G) \geqslant 2g - 1$.

Now we are ready to describe the construction.

Let $T$ be a subset of $\mathscr{X}(\mathbf{F}_q)$; i.e., $T$ is a set of $\mathbf{F}_q$-rational points of $\mathscr{X}$. Let $G$ be a divisor with $T \cap \operatorname{Supp}(G) = \varnothing$. Each point $P \in T$ can be associated with a map $h_P$ from $\mathscr{L}(G)$ to $\mathbf{F}_q$ defined by

$$h_P(f) = f(P).$$

LEMMA 3.1. *Let* $\mathscr{H} = \{h_P \mid P \in T\}$. *If* $\deg(G) \geqslant 2g + 1$, *then the cardinality of* $\mathscr{H}$ *is equal to* $|T|$.

*Proof.* It is sufficient to prove that $\{h_P\}_{P \in T}$ are pairwise distinct. Assume that $h_P = h_Q$ for $P$ and $Q$ in $T$, i.e.,

$$h_P(f) = h_Q(f) \tag{6}$$

for all $f \in \mathscr{L}(G)$. This is equivalent to the fact that

$$f(P) = f(Q) \tag{7}$$

for all $f \in \mathscr{L}(G)$.

Suppose that $P$ is different from $Q$. As $\deg(G - P) > \deg(G - P - Q) \geqslant 2g - 1$, we obtain by the Riemann–Roch theorem

$$\ell(G - P) = \deg(G) - g, \qquad \ell(G - P - Q) = \deg(G) - g - 1.$$

By the above results on dimensions, we can choose a function $u$ from the set $\mathscr{L}(G - P) - \mathscr{L}(G - P - Q)$. Then it is clear that $u(P) = 0$ and $u(Q) \neq 0$. This contradicts (7). Hence $P = Q$. The proof is complete.

THEOREM 3.1. *Let* $\mathscr{X}/\mathbf{F}_q$ *be an algebraic curve and* $T$ *a set of* $\mathbf{F}_q$*-rational points of* $\mathscr{X}$. *Suppose that* $G$ *is a divisor with* $\deg(G) \geqslant 2g + 1$ *and* $T \cap \operatorname{Supp}(G) = \varnothing$. *Then there exists a perfect hash family* $PHF(|T|; q^{\deg(G) - g + 1}, q, w)$ *if* $|T| > \deg(G) \times \binom{w}{2}$.

*Proof.* Let $\mathscr{H}$ be as the above. For a subset $X$ of $\mathscr{L}(G)$ with $w$ elements, consider the set

$$\mathscr{S}_X := \{(u-v)^2 \mid u \neq v \in X\}.$$

Then $\mathscr{S}_X$ has at most $\binom{w}{2}$ elements and the number of zeros of an element $(u-v)^2$ is equal to the number of zeros of $u-v$, which is at most $\deg(G)$ since $u-v$ is an element of $\mathscr{L}(G)$. Therefore, the number of zeros of all functions in $\mathscr{S}_X$ is at most

$$\deg(G) \times |\mathscr{S}_X| \leqslant \deg(G) \times \binom{w}{2}.$$

By the condition $|T| > \deg(G) \times \binom{w}{2}$, we can find a point $R \in T$ such that $R$ is not a zero for any functions of $\mathscr{S}_X$.

We claim that the function $h_R$ is one-to-one on the subset $X$. In fact, suppose $u$ and $v$ are two different elements of $X$. Then $(u-v)^2 \in \mathscr{S}_X$, thus $R$ is not the zero of $(u-v)^2$, i.e., $u(R) \neq v(R)$. This is equivalent to $h_R(u) \neq h_R(v)$. The proof is completed.

Theorem 3.1 gives a construction of perfect hash families based on general algebraic curves over finite fields. In the examples below, we apply Theorem 3.1 to some special curves to obtain some families with nice parameters.

EXAMPLE 3.1. Consider the projective line $\mathscr{X}/\mathbf{F}_q$. Then $g = g(\mathscr{X}) = 0$. Let $N$ be an integer between 2 and $q+1$, and $t, w$ be two positive integers satisfying $N > t\binom{w}{2}$. Then there exists a subset $T$ of rational points of $\mathscr{X}$ with $|T| = N$ and a divisor $G$ of degree $t$ with $T \cap \mathrm{Supp}(G) = \varnothing$. Applying Theorem 3.1 gives a $PHF(N; q^{t+1}, q, w)$. Taking $N = q+1$, we obtain a $PHF(q+1; q^t, q, w)$ provided $q+1 > t\binom{w}{2}$. In particular, a very special case is the existence of a $PHF(q+1; q^2, q, w)$ for $q+1 > \binom{w}{2}$ (also see [3, Corollary 3.2] for this special case).

EXAMPLE 3.2. Let $q = p^u$ for a prime $p$. Put

$$N_q(1) = \begin{cases} q + \lfloor 2\sqrt{q} \rfloor & \text{if } \ p \mid \lfloor 2\sqrt{q} \rfloor \text{ and } u \geqslant 3 \\ q + \lfloor 2\sqrt{q} \rfloor + 1 & \text{otherwise,} \end{cases}$$

where $\lfloor \cdot \rfloor$ denotes the integral part of a real number. It is proved in [18] that there exists an elliptic curve $\mathscr{X}/\mathbf{F}_q$ with $N_q(1)$ rational points.

Let $N$ be an integer between 2 and $N_q(1)$, and $t, w$ be two positive integers with $t \geqslant 3$ and $N > t\binom{w}{2}$. Then there exists a subset $T$ of rational

points of $\mathscr{X}$ with $|T| = N$ and a divisor $G$ of degree $t$ such that $T \cap \mathrm{Supp}(G) = \varnothing$. Applying Theorem 3.1 gives a $PHF(N; q^t, q, w)$ since $g = g(\mathscr{X}) = 1$. In particular, there exists a $PHF(N_q(1); q^t, q, w)$ if $N_q(1) > t\binom{w}{2}$.

EXAMPLE 3.3. Let $q$ be a square and put $r = \sqrt{q}$. Consider the Hermitian curve $\mathscr{X}/\mathbf{F}_q$ defined by

$$y^r + y = x^{r+1}.$$

Then the number of $\mathbf{F}_q$-rational points of $\mathscr{X}$ is equal to $r^3 + 1 = q\sqrt{q} + 1$ and the genus of $\mathscr{X}$ is $g = \sqrt{q}(\sqrt{q} - 1)/2$. Let $N$ be an integer between $\sqrt{q}(\sqrt{q} - 1) + 2$ and $q\sqrt{q} + 1$, and $t, w$ be two positive integers with $t \geqslant \sqrt{q}(\sqrt{q} - 1) + 1$ and $N > t\binom{w}{2}$. Then there exists a subset $T$ of rational points of $\mathscr{X}$ with $|T| = N$ and a divisor $G$ of degree $t$ such that $T \cap \mathrm{Supp}(G) = \varnothing$. Applying Theorem 3.1 gives a $PHF(N; q^{t+1-\sqrt{q}(\sqrt{q}-1)/2}, q, w)$. In particular, there exists a $PHF(q\sqrt{q} + 1; q^{t+1-\sqrt{q}(\sqrt{q}-1)/2}, q, w)$ if $q\sqrt{q} + 1 > t\binom{w}{2}$.

Next, we give an explicit construction based on the Garcia–Stichtenoth curves. Let $q$ be a square and put $r = \sqrt{q}$. Consider a sequence of algebraic curves $\mathscr{X}_i$ given in [13] as follows. Let $\mathscr{X}_1$ be the projective line with the function field $\mathbf{F}_q(\mathscr{X}) = \mathbf{F}_q(x_1)$. Let $\mathscr{X}_i$ be obtained by adjoining a new equation,

$$x_i^r + x_i = \frac{x_{i-1}^r}{x_{i-1}^{r-1} + 1},$$

for all $i \geqslant 2$. Then the number of $\mathbf{F}_q$-rational points of $\mathscr{X}_i$ is more than $(r^2 - r)\, r^{i-1}$, and the genus $g_i$ of $\mathscr{X}_i$ is less than $r^i$ for all $i \geqslant 1$.

Put

$$N_i = (r^2 - r)\, r^{i-1} = (\sqrt{q} - 1)\, q^{i/2}, \qquad t_i = \lfloor (c+1)\, r^i \rfloor = \lfloor (c+1)\, q^{i/2} \rfloor,$$

$$w = \left\lfloor \sqrt{\frac{2}{c+1}}\, q^{1/4} \right\rfloor,$$

where $c \geqslant 1$ is a real constant independent of $i$. Then

$$N_i > t_i \binom{w}{2} \qquad \text{for all} \quad i \geqslant 1,$$

and there exist a subset $T_i$ of rational points of $\mathscr{X}_i$ with $|T_i| = N_i$, a divisor $G_i$ of degree $t_i$ of $\mathscr{X}_i$ such that $T_i \cap \mathrm{Supp}(G_i) = \varnothing$. Applying Theorem 3.1

gives $PHF(N_i; q^{t_i+1-g_i}, q, w)$ for all $i \geqslant 1$. Since $N_i = (\sqrt{q}-1)\, q^{i/2}$, $w = \lfloor \sqrt{\frac{2}{c+1}}\, q^{1/4} \rfloor$ and $t_i + 1 - g_i \geqslant \lfloor (c+1)\, r^i \rfloor + 1 - r^i > \lfloor cq^{i/2} \rfloor$, we have

THEOREM 3.2. *Let the prime power $q$ be a square and let $c \geqslant 1$ be a real number. Then there exists a*

$$PHF\left( (\sqrt{q}-1)\, q^{i/2}; q^{\lfloor cq^{i/2} \rfloor}, q, \left\lfloor \sqrt{\frac{2}{c+1}} q^{1/4} \right\rfloor \right)$$

*for each $i \geqslant 1$. In particular, taking $c = 1$, we obtain a*

$$PHF((\sqrt{q}-1)\, q^{i/2}; q^{q^{i/2}}, q, \lfloor q^{1/4} \rfloor)$$

*for all $i \geqslant 1$.*

Before describing the next result, we first recall a simple product construction of perfect hash families, due to Blackburn *et al.* [5, 4]. Assume that $\mathscr{H}_1$ is a $PHF(N; n, n_0, w)$ from $A_1$ to $B_1$ and $\mathscr{H}_2$ is a $PHF(N_0; n_0, m, w)$ from $A_2$ to $B_2$ such that $B_1 = A_2$. Then it is fairly straightforward to verify that $\mathscr{H} = \{h_2 h_1 \mid h_1 \in \mathscr{H}_1, h_2 \in \mathscr{H}_2\}$ is a $PHF(NN_0; n, m, w)$ from $A_1$ to $B_2$. That is,

LEMMA 3.2 [4]. *Suppose there exist explicit $PHF(N; n, n_0, w)$ and $PHF(N_0; n_0, m, w)$. Then there exists an explicit $PHF(NN_0; n, m, w)$.*

Combining Theorem 3.2 with Lemma 3.2, we are ready to prove our main result in the paper.

THEOREM 3.3. *For any integers $m \geqslant w$, there exist explicit constructions of $PHF(N; n, m, w)$ such that $N = C\log n$, where $C$ is a constant independent of $n$, and $n$ can go to $\infty$.*

*Proof.* Let $m \geqslant w$ be two integers. Let $q$ be the least square prime power such that $q \geqslant m$ and $q^{1/4} \geqslant w$. Since $g(x) = \sqrt{(2/(x+1))}\, q^{1/4}$ is continuous on $[1, \infty)$, it follows that we may choose a $c_0 \in [1, \infty)$ such that $\sqrt{(2/(c_0+1))}\, q^{1/4} = w$. By Theorem 3.2, we know that there is an explicit $PHF((\sqrt{q}-1)\, q^{i/2}; q^{\lfloor c_0 q^{i/2} \rfloor}, q, w)$ for all $i \geqslant 1$. Since $q \geqslant m$, there exists an explicit $PHF(N_0; q, m, w)$, where the parameter $N_0$ can be effectively determined by $m$ because of the previous choice of $q$. From Lemma 3.2, it follows that there exist constructions for

$$PHF(N_0(\sqrt{q}-1)\, q^{i/2}; q^{\lfloor c_0 q^{i/2} \rfloor}, m, w)$$

for all $i \geqslant 1$. We thus obtain $PHF(N, n, m, w)$ with $N = C \log n$, where

$$C \approx \frac{N_0(\sqrt{q} - 1) \log q}{c_0}$$

in which all the parameters of the right-hand side in the equation depend only on $m$ and $w$, but $n$ can go to $\infty$ as $n = q^{\lfloor c_0 q^{i/2} \rfloor}$ for all $i = 1, 2, \ldots$. The desired result follows.

## 4. EXAMPLES

In this section, we exhibit examples to illustrate the efficiency of our constructions in the previous section.

Consider $PHF(N; n, m, w)$ with $m = w = 3$. Atici *et al.* [3] gave an explicit construction of $PHF(3 \times 4^j; 5^{2^j}, 3, 3)$ for any integer $j \geqslant 1$; this results in a $PHF(N; n, 3, 3)$ with $N \approx 0.556(\log n)^2$.

Now we look at our construction. Let $q = 3^4$. From Theorem 3.2 we have an explicit construction of $PHF(8 \times 3^{2i}; 3^{4 \times 3^{2i}}, 3^4, 3)$ for all $i \geqslant 1$. We also know that there exist constructions for $PHF(2k^2 - 2k; k^3, 3, 3)$ for all $k \geqslant 2$ [3, Corollary 5.2]. Taking $k = 4$, we obtain a $PHF(56; 3^4, 3, 3)$. Applying Theorem 3.3, we have an explicit $PHF(N; n, 3, 3)$ with $N = 56 \times 8 \times 3^{2i}$, $n = 3^{4 \times 3^{2i}}$ for each $i \geqslant 1$. It follows

$$N = \frac{56 \times 8}{4 \times \log 3} \log n \approx 70.664 \log n.$$

Thus the asymptotic behavior of our construction as $n \to \infty$ is much better than that from [3].

Another useful example is to look at the applications of perfect hash families to the constructions of cover-free families.

Recall that a set system $(X, \mathscr{B})$ with $X = \{x_1, \ldots, x_v\}$ and $\mathscr{B} = \{B_i \subseteq X \mid i = 1, \ldots, \ell\}$ is called a $(v, \ell, t)$-*cover-free family* (or $(v, \ell, t)$-CFF for short) if for any subset $\Delta \subseteq \{1, \ldots, \ell\}$ with $|\Delta| = t$ and any $i \in \Delta$,

$$\left| B_i \setminus \bigcup_{\substack{j \in \Delta \\ j \neq i}} B_j \right| \geqslant 1.$$

The elements of $X$ are called *points* and elements of $\mathscr{B}$ are called *blocks*. In other words, in a $(v, \ell, t)$-CFF $(X, \mathscr{B})$ the union of any $t - 1$ blocks in $\mathscr{B}$ can not cover any other remaining one.

Cover-free families were first introduced in 1964 by Kautz and Singleton [15] in terms of superimposed binary codes. They have found many applications to information theory, combinatorics, communication and

cryptography. Constructing $(v, \ell, t)$-CFF with maximal $\ell$ for given $v$ and $t$ has been considered by numerous authors (see, for example, [1, 9, 10, 14, 17, 20, 21]).

In [10], Erdős *et al.* showed that for given $\ell$ there exist $(v, \ell, t)$-CFF with $v = O(t^2 \log \ell)$. This result is, however, non-constructive and explicit constructions with good asymptotic behavior are desirable. In a similar situation as the perfect hash families, little is known about asymptotically good and explicit constructions. Using our explicit results on perfect hash families, we are able to obtain explicit constructions for $(v, \ell, t)$-CFF in which $v$ is $O(t^4 \log \ell)$. This is again among the most efficient, explicit constructions for CFFs in the literature.

The connections between perfect hash families and cover-free families have been implicitly studied by Stinson *et al.* [20]. Assume that $\mathscr{H}$ is a $PHF(N; n, m, w)$ from $A$ to $B$. Let $A = \{1, 2, ..., n\}$ and $B = \{1, 2, ..., m\}$. We define

$$X = \mathscr{H} \times B = \{(h, j) \mid h \in \mathscr{H}, j \in B\}.$$

For each $1 \leqslant i \leqslant n$, we define a subset (block) $B_i$ of $X$ by

$$B_i = \{(h, h(i)) \mid h \in \mathscr{H}\},$$

and $\mathscr{B} = \{B_i \mid 1 \leqslant i \leqslant n\}$. Then $(X, \mathscr{B})$ is a $(Nm, n, w)$-CFF. Clearly, $|X| = Nm$ and $|\mathscr{B}| = n$. For any $w$ blocks $B_{i_1}, ..., B_{i_w}$, since $\mathscr{H}$ is a $PHF(N; n, m, w)$, there exists a perfect hash function $h \in \mathscr{H}$ such that $h$ restricted on $\{i_1, ..., i_w\}$ is one-to-one. It follows that $h(i_1), ..., h(i_w)$ are $w$ distinct elements in $B$, which also implies that $(h, h(i_1)), ..., (h, h(i_w))$ are $w$ distinct elements in $B_{i_1}, ..., B_{i_w}$, respectively. So the union of any $w-1$ blocks in $\mathscr{B}$ cannot cover the remaining one; the desired result follows. We have

THEOREM 4.1. *If there exists a $PHF(N; n, m, w)$, then there exists an $(Nm, n, w)$-CFF.*

Applying Theorem 3.3, we immediately obtain the following result.

COROLLARY 4.1. *For any $\ell$, there exists an explicit construction for $(v, \ell, t)$-CFF in which $v$ is $O(t^4 \log \ell)$.*

In particular, considering the above mentioned example of a $PHF(N; n, 3, 3)$ with $N \approx 70 \log n$, we get an explicit construction of $(v, \ell, 3)$-CFF with $v \approx 210 \log \ell$. Erdős *et al.* show in [10] that for any $(v, \ell, 3)$-CFF, one has $v \geqslant \lceil 3.1 \log \ell \rceil$. Dyer *et al.* [9] give a probabilistic construction with $v = \lceil 13 \log \ell \rceil$. Our explicit construct increases the parameter $v$ around 16 times from the best known probabilistic construction.

## 5. CONCLUSIONS

In this paper we give explicit constructions of perfect hash families from algebraic curves with many rational points. We show that for any integers $m$ and $w$, there exist infinite classes of explicit $PHF(N; n, m, w)$ with $N = O(\log n)$, which are more efficient explicit constructions than those having already appeared in the literature. We show that such perfect hash families can be used to construct explicit cover-free families that are also not known previously.

Finally, it is worth pointing out that the perfect hash families constructed from the algebraic curves are all linear. Linear perfect hash families are recently introduced by Blackburn and Wild [6]. A perfect hash family $\mathscr{H}$ from $A$ to $B$ is called *linear* if $B$ is identified with a finite field and $A$ with a vector space over $B$. The authors in [6] show that for integers $d$ and $w$ such that $d \geqslant 2$ and $w \geqslant 2$ and $q$ a prime power, a linear $PHF(N; q^d, q, w)$ exists only if $N \geqslant d(w-1)$. They also give an optimal linear $PHF(N; q^d, w)$ with $N = d(w-1)$. However, their explicit construction requires that $q$ is very large compared to $d$ and $w$, that is, $q \geqslant (\frac{1}{2}t(w-1))^{d(w-1)}$. It is straightforward to verify that our constructions based on the algebraic curves over finite field are all linear. From Theorem 3.8, we know that for any square prime power $q$ and $w = O(q^{1/4})$, there exist linear $PHF(N; n, q, w)$ with $N = O(\log n)$.

## REFERENCES


1. N. Alon, Explicit construction of exponential sized families of $k$-independent sets, *Discrete Math.* **58** (1986), 191–193.
2. N. Alon and M. Naor, Derandomization, witnesses for Boolean matrix multiplication and construction of perfect hash functions, *Algorithmica*, **16** (1996), 434–449.
3. M. Atici, S. S. Magliveras, D. R. Stinson, and W. D. Wei, Some recursive constructions for perfect hash families, *J. Combin. Des.* **4** (1996), 353–363.
4. S. R. Blackburn, Combinatorics and threshold cryptology, *in* "Combinatorial Designs and Their Applications," CRC Research Notes in Mathematics, pp. 49–70, CRC Press, London, 1999.
5. S. R. Blackburn, M. Burmester, Y. Desmedt, and P. R. Wild, Efficient multiplicative sharing schemes, *in* "Advance in Cryptology-Eurocrypt '96," Lecture Notes in Comput. Sci., Vol. 1070, pp. 107–118, Springer-Verlag, New York/Berlin, 1996.
6. S. R. Blackburn and P. R. Wild, Optimal linear perfect hash families, *J. Combin. Theory Ser. A* **83** (1998), 233–250.
7. E. F. Brickell, A problem in broadcast encryption, *in* "5th Vermont Summer Workshop on Combinatorics and Graph Theory, June 1991."
8. Z. J. Czech, G. Havas, and B. S. Majewski, Perfect hashing, *Theoret. Comput. Sci.* **182** (1997), 1–143.
9. M. Dyer, T. Fenner, A. Frieze, and A. Thomason, On key storage in secure networks, *J. Cryptology* **8** (1995), 189–200.

10. P. Erdős, P. Frankl, and Z. Furedi, Families of finite sets in which no set is covered by the union of $r$ others, *Israel J. Math.* **51** (1985), 79–89.
11. A. Fiat and M. Naor, Broadcast encryption, *in* "Advances in Cryptology-Crypto '93," Vol. 773, pp. 480–491, Springer-Verlag, New York/Berlin, 1994.
12. M. L. Fredman and J. Komlòs, On the size of separating systems and families of perfect hash functions, *SIAM J. Algebraic Discrete Methods* **5** (1984), 61–68.
13. A. Garcia and H. Stichtenoth, On the asymptotic behavior of some towers of function fields over finite fields, *J. Number Theory*, **61** (1996), 248–273.
14. L. Gong and D. J. Wheeler, A matrix key-distribution scheme, *J. Cryptology* **2** (1990), 51–59.
15. W. H. Kautz and R. C. Singleton, Nonrandom binary superimposed codes, *IEEE Trans. Inform. Theory* **10** (1964), 363–377.
16. K. Mehlhorn, "Data Structures and Algorithms," Vol. 1, Springer-Verlag, New York/Berlin, 1984.
17. C. J. Mitchell and F. C. Piper, Key storage in secure networks, *Discrete Appl. Math.* **21** (1988), 215–228.
18. J.-P. Serre, Rational points on curves over finite fields, lecture notes, Harvard University, 1985.
19. H. Stichtenoth, "Algebraic Function Fields and Codes," Springer-Verlag, Berlin, 1993.
20. D. R. Stinson, T. van Trung, and R. Wei, Secure frameproof codes, key distribution patterns, group testing algorithms and related structures, *J. Statist. Plann. Inference*, in press.
21. D. S. Stinson, R. Wei, and L. Zhu, New constructions for perfect hash families and related structures using combinatorial designs and codes, *J. Combin. Des.*, in press.
22. M. A. Tsfasman and S. G. Vlădut, "Algebraic-Geometric Codes," Kluwer Academic, Dordrecht, 1991.